

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew J. Schrauger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, with any iCloud accounts associated with telephone number 602-459-3573 that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Homeland Security Investigations (HSI) in Nogales, Arizona and have been so employed since May 2021. As such, I am an investigative law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. Prior to joining HSI, I was employed as a Border Patrol Agent in Tucson, Arizona and since 2011 to 2021.

3. As a Special Agent for HSI, I am responsible for investigating laws enumerated in Title 8, Title 18, and Title 21 of the United States Code. Included in my responsibilities are the investigation of illicit contraband-smuggling, including narcotics smuggling, across the United States border. In preparing to become a Special Agent, I attended the Basic Criminal Investigator

and the HSI Special Agent training programs at the Federal Law Enforcement Training Center in Glynco, Georgia.

4. During my career in law enforcement, I have participated in multiple investigations involving illegal drugs, bulk cash smuggling, and weapons. During these investigations, I have been involved in seizures of cocaine, heroin, methamphetamine, fentanyl, and other illicit or controlled substances. I have assisted in the interrogation of numerous subjects/defendants involved in and/or arrested for drug and narcotics violations. I also participated in several joint interagency federal and state investigations. In the course of these investigations, I conducted thorough background checks of targets, conducted physical surveillance, and monitored and reviewed recorded conversations of drug traffickers.

5. I have also gained experience in the common practices of drug traffickers through conducting several controlled substances investigations and assisting in a similar number of investigations being conducted by other agents. In preparation for this affidavit, I have consulted with senior agents of HSI. These senior agents have additional experience in conducting complex drug investigations including international conspiracies, money laundering activities and related electronic evidence.

6. I know, based upon training, experience, and the experience of other senior agents, as well as from information relayed to me during the course of my official duties, that a significant percentage of methamphetamine, heroin, cocaine, and fentanyl imported into the United States are currently entering the domestic market at various points along the Southwest border of the United States. Furthermore, I know that several well-organized and sophisticated organizations control the importation and initial distribution of methamphetamine, heroin, cocaine, and fentanyl. I have also learned, based upon training, experience, and the experience

of other senior agents, that Mexican Drug Trafficking Organizations (DTOs) transport cash proceeds generated from the sale of illegal controlled substances back to the Southwest border of the United States where the currency is remitted to Mexico via wire transfers, money orders, or currency-laden vehicles.

7. I know that these drug trafficking and money laundering organizations routinely utilize several operational techniques to sustain their illegal enterprise. These practices are designed and implemented to achieve two paramount goals: first, the successful facilitation of the organization's illegal activities which consists of the importation and distribution of illegal controlled substances and the subsequent repatriation of the proceeds of that illegal activity; and second, minimization of the exposure of organization members, particularly those operating in management roles, from investigation and prosecution by law enforcement.

8. I know that the more entrenched and sophisticated trafficking organizations routinely compartmentalize their illegal operations. The compartmentalization of operations reduces the amount of knowledge possessed by each member of the organization. This method of operation effectively minimizes the potential damage a cooperating individual could inflict on the organization and further reduces the adverse impact of a particular law enforcement action against the organization. However, in order to effectively manage and coordinate the illegal activities, the upper management of the organization must maintain regular contact with each compartment.

9. I know that the aforementioned Mexican DTOs have evolved to a level of sophistication where virtually every phase of their illegal activities is conducted as a separate operation. I have learned that major Mexican DTOs employ various sub-organizations or “cells”

that independently accomplish tasks, such as: the receipt and transportation of illegal drugs in and through Mexico; the importation of illegal drugs into the United States; the storage of illegal drugs along the Southwest border in the United States; the transportation of illegal drugs from the Southwest border to destination markets in the United States; the transportation of cash proceeds from the destination markets to the Southwest border and Mexico; the laundering of cash proceeds in the United States and Mexico; the repatriation of cash proceeds to the original owners of the drugs in Mexico and/or South America; the establishment of both “front” and legitimate companies; and real estate acquisitions in the United States and Mexico. Finally, I have learned in the most compartmentalized organizations, there is often limited contact among the “cells.”

10. I know that these drug trafficking and money laundering organizations routinely utilize different methods of counter surveillance to facilitate the illegal activities of the DTO including the use of scouts and sophisticated communications network.

11. In the course of conducting drug investigations, I have personally interviewed persons involved in the distribution of illegal drugs. In addition, I have provided surveillance support in state and federal investigations. I have searched cellular telephones and “smart phones” and identified evidence of illegal activities. I have experience concerning the practices of drug traffickers and the best methods of investigating them.

12. Members of these organizations routinely utilize electronic communications facilities including cellular telephones and text messaging to communicate with other organization members in furtherance of their illegal goals. During the course of these electronic

communications, organization members commonly use coded language and references and/or encryption in an effort to elude law enforcement detection.

13. I know, based upon training and experience, that the communication of time sensitive information is critical to the success of these organizations' illegal activities. The critical nature of this information stems from the necessity of the organization's management to provide direction for the importation and distribution of controlled substances, as well as the subsequent laundering of the proceeds of those illegal activities.

14. The statements contained in this affidavit are based on my experience and background as a law enforcement officer and, in part, on information provided by other law enforcement officers, records obtained by those officers and corresponding summaries. I am familiar with the information submitted in this affidavit. As this affidavit is submitted for a limited purpose, it does not recite all aspects of this investigation, but only sufficient information to establish probable cause in support of the issuance of this search warrant.

15. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 21 U.S.C. §846, §841(a)(1), §841(b)(1)(A)(vi), §963, §952(a), §960(a)(1), and §960(b)(1)(F), as described in Attachment B.

JURISDICTION

16. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A) and (d). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). As discussed more

fully below, the acts or omissions in furtherance of the offenses under investigation occurred within the District of Arizona. See 18 U.S.C. § 3237.

PROBABLE CAUSE

17. On November 13, 2022, Kaitlan BRUMLEY entered the United States from the Republic of Mexico at the DeConcini Port of Entry in Nogales, Arizona via the vehicle lanes. BRUMLEY was the driver and registered owner of a 2006 Jeep Commander bearing Arizona license plate SGA23K. Diego MENDOZA-Demarbiuex was the passenger sitting in the front seat.

18. During a post-primary inspection, a Canine Enforcement Officer (deployed his Narcotics Human Detection Dog (NHDD) to conduct a canine sniff of BRUMLEY's vehicle. The NHDD alerted to a trained odor emanating from the driver's side undercarriage of BRUMLEY's vehicle.

19. In the secondary inspection area, a Customs and Border Protection Officer (CBPO) asked BRUMLEY where they were coming from, to which BRUMLEY said "California" but quickly corrected herself and said Nogales, Sonora.

20. A CBPO asked BRUMLEY and MENDOZA if they visited anyone in Nogales, Sonora, Mexico. At the same time, BRUMLEY said "no one" and MENDOZA said "yes, a grandmother." BRUMLEY then raised her voice and stated, "we went to visit my grandmother."

21. BRUMLEY and MENDOZA told the CBPO they stayed in Mexico over the weekend, and they were heading to Tucson, Arizona. BRUMLEY told the CBPO she was the registered owner.

22. The CBPO received an oral, negative customs declaration that included narcotics, prescription drugs, or \$10,000 or more in currency.

23. The vehicle was scanned by the Z-Portal, a non-intrusive X-ray, where a certified CBPO observed anomalies in the gas tank and front frame.

24. Upon further inspection, CBPOs discovered a non-factory compartment molded around the gas tank.

25. Inside the non-factory compartment, CBPOs could visually see multiple bags containing blue pills.

26. CBPOs inspected the anomalies by the front frame of BRUMLEY's vehicle and discovered a non-factory compartment. Inside the compartment CBPOs discovered more clear bags containing blue pills.

27. CBPOs seized a total of 238 packages containing suspected fentanyl pills. The suspected fentanyl pills weighed 31.86 kilograms. A sample blue pill was tested using a Rapid Response Kit and tested positive for the properties of fentanyl.

28. On November 15, 2022, samples of the suspected fentanyl were taken to Laboratory and Science Services (LSS) at the Mariposa Port of Entry for preliminary testing and the results were positive for the properties of fentanyl.

29. During a post-Miranda interview of BRUMLEY, she stated that she does not know anybody in Nogales, Sonora, Mexico. BRUMLEY stated both she and MENDOZA slept in BRUMLEY's vehicle over the entire weekend. BRUMLEY specifically stated that they did not stay in a hotel at all during their visit to Nogales, Sonora, Mexico. BRUMLEY stated she and MENDOZA were together the entire time.

30. BRUMLEY then stated she did stop by her grandmother's house but did not actually see her grandmother during the trip.

31. BRUMLEY stated that she is the registered owner of the Jeep Commander and paid approximately \$1,500 USD for the vehicle a few months ago.

32. BRUMLEY stated she was with the vehicle the entire visit except on one occasion when she and MENDOZA went into an abandoned building.

33. During a post-Miranda interview of MENDOZA, he stated that they went to BRUMLEY's grandmother's house Nogales, Sonora, Mexico, but agreed to find a hotel nearby.

34. MENDOZA stated that BRUMLEY paid for the hotel.

35. MENDOZA stated that he remained at the hotel on Saturday November 12, 2022, all day while BRUMLEY went out and explored. MENDOZA stated that BRUMLEY did not return until approximately 9:00 PM.

36. MENDOZA stated that they physically saw BRUMLEY's grandmother during their trip.

37. BRUMLEY's cellular phone was receiving alerts during the interview. Multiple notifications in multiple text applications were identified. Also, multiple missed phone calls were identified. It is common in my training and experience that coconspirators will repeatedly contact the driver of a load of narcotics around the time a load driver is crossing the border. This is done to both check on if the load of narcotics was successfully smuggled across the border and to coordinate a meeting where the narcotics can be offloaded. A search warrant would allow agents to further examine these incoming messages and calls to potentially identify coconspirators and locations being used to offload or transfer narcotics.

38. Record checks performed on BRUMLEY revealed she is a citizen of the United States. BRUMLEY has only two other border crossings. Those occurred on October 16, 2022, and October 3, 2022.

39. BRUMLEY's cellular phone was in her possession when she was apprehended

40. Based on my training, experience, and responses to multiple port cases that co-conspirators will often contact narcotics load carriers throughout their smuggling attempts. These co-conspirators will often maintain communication with the load carrier in order to check the status and location of the load. BRUMLEY received multiple calls and messages on November 13, 2022, at the time she attempted to cross through the POE.

41. I know that Apple iOS devices often store and backup user data to iCloud. I know that WhatsApp data can also be enabled by the user of an iOS device to store and backup data to iCloud. WhatsApp is an application that can be installed on iOS devices and allows one or more users to communicate via secured encryption.

42. On December 21, 2022, a search warrant was issued by U.S. Magistrate Judge Eric J. Markovich for the mobile device seized from BRUMLEY on the day of her arrest. (United States District Court Case No. 22-00799MB.)

43. The warrant for BRUMLEY'S cellular phone was executed on December 22, 2022. Special Agent Richard Koch was unable to extract any electronic data due to phone security features preventing agents from being able to do a full extraction. The partial extraction of BRUMLEY'S iPhone also included various account information to include BRUMLEY'S cellular phone number, 602-459-3573.

INFORMATION REGARDING APPLE ID AND iCloud¹

44. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

45. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or

through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

46. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

47. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

48. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the

length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

49. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

50. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be

captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

51. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

52. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

53. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

54. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

55. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

56. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of applications downloaded from the App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators such as different third-party applications used to facilitate banking or other financial activity or third-party applications that are used to facilitate communication that may be encrypted. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

57. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

59. Based on the forgoing, I request that the Court issue the proposed search warrant.

60. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

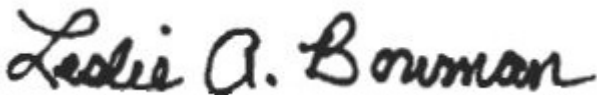
61. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,
**MATTHEW J
SCHRAUGER**

Digitally signed by MATTHEW J
SCHRAUGER
Date: 2023.03.08 20:12:36 -07'00'

Matthew J. Schrauger
Special Agent
Homeland Security Investigations (HSI)

Subscribed and sworn to telephonically this 9th day of March, 2023



Honorable Leslie A. Bowman
United States Magistrate Judge